WHAT IS CLAIMED IS:

1. In a data processing system, a method for updating a utility, comprising the steps of:

receiving a request to unlock the utility;

verifying an update to the utility; and

using a system management interrupt (SMI) handler to query a status of the verifying step.

2. The method as recited in claim 1, further comprising the step of:

if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility.

3. The method as recited in claim 1, further comprising the step of:

not unlocking the utility if the verifying step fails to verify the update to the utility.

4. The method as recited in claim 2, wherein the verifying step is performed by a trusted platform module (TPM) in accordance with Trusted Computing Platform Alliance Specifications.

5. The method as recited in claim 4, wherein the SMI handler used to query the status of the verifying step queries the TPM for the status.

6. The method as recited in claim 5, wherein the SMI handler is issued by the TPM.

7. The method as recited in claim 2, further comprising the step of: after the utility has been updated, locking the utility with the SMI handler.

8. The method as recited in claim 1, wherein the utility is a flash utility.

9. The method as recited in claim 2, wherein the requesting step is performed by an SMI handler.

10. A computer program product adaptable for storage on a computer readable medium and operable for updating a utility, comprising:

programming for receiving a request to unlock the utility;

programming for verifying an update to the utility; and

programming for using a system management interrupt (SMI) handler to query a status of the verifying programming.

11. The computer program product as recited in claim 10, further comprising:

if the verifying programming successfully verifies the update of the utility, programming for unlocking the utility and updating the utility.

12. The computer program product as recited in claim 10, further comprising:

programming for not unlocking the utility if the verifying programming fails to verify the update to the utility.

13. The computer program product as recited in claim 11, wherein the verifying programming is performed by a trusted platform module (TPM) in accordance with Trusted Computing Platform Alliance Specifications.

14. The computer program product as recited in claim 13, wherein the SMI handler used to query the status of the verifying programming queries the TPM for the status.

15. The computer program product as recited in claim 14, wherein the SMI handler is issued by the TPM.

16. The computer program product as recited in claim 11, further comprising:

after the utility has been updated, programming for locking the utility with the SMI handler.

17. The computer program product as recited in claim 11, wherein the requesting programming is performed by an SMI handler.

09934550.094601

18. A data processing system comprising:

a processor;

a trusted platform module (TPM) coupled to the processor and operating under Trusted Computing Platform Alliance Specifications;

a BIOS utility stored in flash memory coupled to the processor;

an input circuit for receiving an update to the BIOS utility; and

a bus system for coupling the input circuit to the processor;

a BIOS update application requesting an unlock of the flash memory from a system management interrupt (SMI) handler;

the SMI handler including programming for requesting cryptographic verification of the BIOS utility update from the TPM;

the TPM including programming for verifying an authenticity of the BIOS utility update;

the TPM including programming for issuing an SMI to query the TPM for a status on the verifying of the authenticity of the BIOS utility update;

the SMI handler unlocking the flash memory if the SMI handler sets the status as successful;

the BIOS update application updating the BIOS utility with the update; and

the SMI handler locking the flash memory after the update of the BIOS utility has completed.

19. A method comprising the steps of:

(a) a BIOS update application requesting an unlock of a flash utility from a system management interrupt (SMI) handler;

(b) determining if a verification of an update to the flash utility is pending;

(c) if verification of the update to the flash utility is not pending, the SMI handler requesting verification of the update to the flash utility from a trusted platform module (TPM) and setting a status flag as pending;

(d) exiting the SMI handler and returning status flag to the BIOS update application;

(e) receiving by the BIOS update application the status flag from the SMI handler;

(f) returning to step (a) if the status flag is set as pending after step (e);

(g) in response to step (c), the TPM verifies the update to the flash utility;

(h) when step (g) is completed, issuing an SMI by the TPM to query if the verification of the update to the flash utility was successful or failed;

(i) setting the status flag as successful if the verification of the update to the flash utility was successful;

(j) setting the status flag as failed if the verification of the update to the flash utility was not successful;

(k) if step (b) determines that verification of the update to the flash utility is still pending, determining if the verification of the update to the flash utility has completed;

(l) if step (k) determines that verification of the update to the flash utility has not completed, setting the status flag as pending;

(m) if step (k) determines that verification of the update to the flash utility has completed, determining if the verification of the update to the flash utility was successful;

(n) if step (m) determines that the verification of the update to the flash utility was not successful, setting the status flag as failed;

(o) if step (m) determines that the verification of the update to the flash utility was successful, the SMI handler unlocking the flash utility and setting the status flag as successful;

(p) performing steps (d) and (e) in response to any of steps (l), (n), or (o);

(q) determining if the status flag is set as successful if after step (e) it is determined that the status flag is not set to pending; and

(r) updating the BIOS with the update to the flash utility and locking the flash utility with the SMI handler if the status flag is determined to be set to successful in step (q).